Windows Networking Tools

The Complete Guide to Management, Troubleshooting, and Security

Gilbert Held

TECHNISCHE
INFORMATIONSBIBLIOTHEK
UNIVERSITÄTSBIBLIOTHEK
HANNOVER

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Contents

CHAPTER 1 INTRODUCTION 1

1.1 The TCP/IP Protocol Suite 1

1.1.1 Applications 2

1.1.1.1 Current Applications 2

1.1.1.2 Emerging Applications 10

1.2 Book Preview 13

1.2.1 Examining the TCP/IP Protocol Suite 13

1.2.2 IP and MAC Addressing 14

1.2.3 Transport Layer Protocols 14

1.2.4 Working with the Command Prompt 15

1.2.5 Windows Built-In Networking Tools 15

1.2.6 Network Monitoring 15

1.2.7 Network Security 15

1.2.8 Efficiency Methods 16

CHAPTER 2 EXAMINING THE TCP/IP PROTOCOL SUITE 17

2.1 ISO Reference Model 17

2.1.1 OSI Reference Model Layers 19

2.1.1.1 Layer 1: The Physical Layer 19

2.1.1.2 Layer 2: The Data Link Layer 19

2.1.1.3 Layer 2 Subdivision 20

2.1.1.4 Layer 3: The Network Layer 20

2.1.1.5 Layer 4: The Transport Layer 22

2.1.1.6 Layer 5: The Session Layer 22

2.1.1.7 Layer 6: The Presentation Layer 23

2.1.1.8 Layer 7: The Application Layer 23

2.1.2 Data Flow 23
2.2 The TCP/IP Protocol Suite 24
2.2.1 The TCP/IP Network Layer 25
2.2.2 IP 25
2.2.2.1 IPv4 Addressing 26
2.2.2.2 IPv6 Addressing 26
2.2.2.3 ARP 27
2.2.2.4 ICMP 27
2.2.3 The Transport Layer 27
2.2.3.1 TCP 27
2.2.3.2 UDP 28
2.2.4 The Application Layer 29
2.3 Data Flow within a TCP/IP Network 30
2.4 Summary 31
Chapter 3 Addressing at Layers 2 and 3 and the Internet Protocol 33
3.1 Data Link Addressing 34
3.1.1 Ethernet Frame Operations 34
3.1.1.1 Basic Ethernet 36
3.1.1.2 Full Duplex and the PAUSE Frame 44
3.1.1.3 vLAN Tagging 46
3.1.1.4 SNAP Frames 48
3.1.1.5 Frame Determination 48
3.2 Fast Ethernet 50
3.2.1 4B5B Coding 50
3.2.2 Delimiters 51
3.2.3 Interframe Gap 51
3.3 Gigabit Ethernet 51
3.3.1 Standards Evolution 52
3.3.1.1 Varieties 52
3.3.2 Frame Format Modifications 55
3.3.2.1 Carrier Extension 55
3.3.2.2 Half-Duplex Use 56
3.3.2.3 Frame Bursting 56
3.3.2.4 Jumbo Frames 57
3.4.10 Gigabit Ethernet 59
3.4.1 Fiber Standards 60
3.4.1.1 10GBASE-SR 60
3.4.1.2 10GBASE-LR 60
3.4.1.3 10GBASE-LRM 60
3.4.1.4 10GBASE-ER 60
3.4.1.5 10GBASE-ZR 61
3.4.1.6 10GBASE-LX4 61
3.4.2 Copper 61
3.4.2.1 10GBASE-CX4 61
3.4.2.2 10GSFP+Cu 62

3.4.2.3 Backplane 10 GBps Ethernet 62
3.4.2.4 10GBASE-T 62
3.5 The IPv4 Header 63
3.5.1 Vers Field 63
3.5.2 Hlen and Total Length Fields 63
3.5.3 Type of Service Field 64
3.5.4 Identification Field 65
3.5.5 Flags Field 66
3.5.6 Fragment Offset Field 66
3.5.7 Time to Live Field 67
3.5.8 Protocol Field 67
3.5.9 Checksum Field 71
3.5.10 Source and Destination Address Fields 71
3.5.11 Options and Padding Fields 71
3.6 IPv4 Addressing 71
3.6.1 Overview 72
3.6.2 Addressing 73
3.6.3 Basic Addressing Scheme 74
3.6.3.1 Address Classes 75
3.6.3.2 Address Formats 76
3.6.3.3 Address Composition and Notation 76
3.6.3.4 Special IPv4 Addresses 77
3.6.3.5 Subnetting and the Subnet Mask 82
3.6.3.6 Classless Networking 90
3.7 The IPv6 Header 91
3.7.1 Ver Field 92
3.7.2 Priority Field 92
3.7.3 Flow Label Field 93
3.7.4 Payload Length Field 93
3.7.5 Next Header Field 93
3.7.6 Hop Limit Field 94
3.7.7 Source and Destination Address Fields 94
3.7.7.1 Address Types 95
3.7.7.2 Address Notation 95
3.7.7.3 Address Allocation 96
3.7.8 Provider-Based Unicast Addresses 97
3.7.9 Multicast Addresses 97
3.7.10 Transporting IPv4 Addresses 98
3.8 ICMP and ARP 99
3.8.1 ICMP 99
3.8.1.1 ICMPv4 99
3.8.1.2 ICMPv6 101
3.8.2 ARP 103
3.8.2.1 LAN Delivery 103
3.8.3 RARP 107

Chapter 4 Transport Layer Protocols 109
4.1 TCP 109
4.1.1 TCP Header 110
4.1.1.1 Source and Destination Port Fields 110
4.1.1.2 Sequence and Acknowledgment Number Fields 114
4.1.1.3 Hlen Field 115
4.1.1.4 Code Bit Field 116
4.1.1.5 Window Field 117
4.1.1.6 Checksum Field 117
4.1.1.7 Urgent Pointer Field 118
4.1.1.8 Options Field 118
4.1.1.9 Padding Field 118
4.1.2 Connection Establishment 118
4.1.2.1 Connection Function Calls 119
4.1.2.2 Port Hiding 119
4.1.2.3 Passive OPEN 120
4.1.2.4 Active OPEN 120
4.1.3 'Ihe Three-Way Handshake 121
4.1.3.1 Overview 121
4.1.3.2 Operation 121
4.1.3.2 The TCP Window 123
4.1.3.3 Avoiding Congestion 125
4.1.4 TCP Retransmissions 127
4.1.5 Session Termination 127
4.2 UDP 128
4.2.1 UDP Header 128
4.2.1.1 Source and Destination Port Fields 129
4.2.1.2 Length Field 129
4.2.1.3 Checksum Field 129
4.2.2 Operation 130
4.2.3 Applications 130

Chapter 5 Working with the Command Prompt 133
5.1 The Command Prompt Location 133
5.1.1 Options 136
5.1.2 Positioning upon Opening 137
5.1.3 Controlling the Command Prompt Window 137
5.2 Working with Function Keys and Commands 138
5.2.1 Function Key Use 139
5.2.2 Repertoire of Commands 139
5.2.2.1 The Help Command 141
5.2.2.2 The CLS Command 144
5.2.3 Controlling Output and Additional Commands 145
5.2.3.1 Redirection Methods 145
5.2.3.2 Other Useful Commands 151

5.2.3.3 Wildcards 156

CHAPTER 6 WINDOWS BUILT-IN NETWORKING TOOLS 159
6.1 Ping 159
6.1.1 Discovery via Ping 162
6.1.2 Ping Options 162
6.1.3 Using the Round-Trip Delay 163
6.2 Tracert 164
6.2.1 Using Tracert 167
6.3 The Pathping Command 167
6.4 The ipconfig Command 170
6.4.2 The Release and Renew Options 173
6.4.3 The Flushdns Option 174
6.4.4 The Displaydns Option 174
6.5 ARP 175
6.5.1 Reverse ARP (RARP) and ARP and IPv6 178
6.6 The Getmac Command 179
6.7 The Netstat Command 181
6.7.1 Command Format 181
6.7.1.1 The -a Switch 181
6.7.1.2 The -b Switch 183
6.7.1.3 The -e and -s Switches 184
6.7.1.4 The -f Switch 185
6.7.1.5 The -n Switch 185
6.7.1.6 The -o Switch 186
6.7.1.7 The -p Switch and Interval Use 186
6.7.1.8 The -r Switch 187
6.7.1.9 The -s Switch 191
6.7.1.10 The -t Switch 191
6.8 The Route Command 191
6.8.1 Command Format 192
6.8.1.1 -f Switch 193
6.8.1.2 -p Switch 193
6.8.1.3 -4 Switch 193
6.8.1.4 -6 Switch 193
6.8.2 Commands Supported 193
6.8.3 The Destination Option 194
6.8.4 Mask and Netmask 194
6.8.5 The Gateway Option 194
6.8.6 The Metric Option 194
6.8.7 The If Interface Option 195
6.8.8 Working with Route 195
6.8.8.1 The IPv4 Routing Table 196
6.8.8.2 The IPv6 Routing Table 197
6.9 The Nslookup Command 199
6.10 The Getmac Command 202
6.11 The Net Command 203

6.11.1 The Net Accounts Command 204
6.11.1.1 Net Accounts Options 204
6.11.2 The Net Computer Option 206
6.11.3 The Net Config Option 206
6.11.4 The Net Continue, Start, and Stop Options 206
6.11.5 The Net File Option 207
6.11.6 The Net Group Option 207
6.11.7 The Net Helpmsg 209
6.11.8 The Net Send Command 209
6.11.9 The Net Localgroup Option 210
6.11.10 The Net Share Command Option 210
6.11.11 The Net Session Command 213
6.11.12 The Net Statistics Command 214
6.11.13 The Net Time Command 217
6.11.14 The Net Use Command 218
6.12 The Net User Command 221
6.13 The Netsh Command 224
6.13.1 The Netsh Wlan Command 228
6.13.1.1 The Add Subcommand 231
6.13.1.2 The Connect Subcommand 233
6.13.1.3 The Delete Subcommand 234
6.13.1.4 The Export Profile Subcommand 236
6.13.1.5 Other Netsh Wlan Functions 238

CHAPTER 7 NETWORK MONITORING WITH WIRESHARK AND WINDUMP 241
7.1 Wireshark 241
7.1.1 Program Evolution 241
7.1.2 Obtaining the Program 242
7.1.3 Program Overview 244
7.1.4 The Capture Screen 246
7.1.4.1 Packet Colors 246
7.1.4.2 Examining a Packet 247
7.1.4.3 File Menu Options 250
7.1.5 Working with Filters 250
7.1.5.1 Filter Expressions 253
7.1.5.2 Applying a Filter 254
7.1.6 Statistics 256
7.1.6.1 Summary Data 256
7.1.6.2 Protocol Hierarchy 257
7.1.6.3 Conversations 257
7.1.6.4 Endpoints 259
7.1.6.5 Packet Lengths 259
7.1.6.6 IO Graphs 259
7.1.6.7 Conversation List 260
7.1.6.8 Endpoint List and Other Entries 260

7.1.7 Telephony 261

7.1.7.1 RTP 261

7.1.7.2 Stream Analysis 263

7.1.7.3 VoIP Calls 265

7.1.8 The Tools Menu 269

7.2 WinDump 269

7.2.1 Overview 270

7.2.1.1 Initial Operation 271

7.2.1.2 Selecting an Interface 271

7.2.1.3 Program Format 273

7.2.1.4 Using Multiple Switches 274

7.2.1.5 Program Switches 276

7.2.2 WinDump Expressions 288

7.2.2.1 Qualifiers 288

7.2.2.2 Expression Primitives 290

7.2.2.3 Relationship Operators 290

7.2.2.4 Utilization Examples 290

CHAPTER 8 NETWORK INTRUSION AND SECURITY 299

8.1 Snort 299

8.1.1 Requirements 300

8.1.2 Installation 302

8.1.3 Commencing Snort 304

8.1.3.1 Sniffer Mode 304

8.1.3.2 Packet Logger Mode 307

8.1.3.3 Network Intrusion Detection System Mode 308

8.1.4 Command Switches 310

8.1.4.1 The -A Switch 310

8.1.4.2 The -b Switch 312

8.1.4.3 The -B Switch 312

8.1.4.4 The -C Switch 314

8.1.4.5 The -d Switch 314

8.1.4.6 The -E Switch 314

8.1.4.7 The -f Switch 314

8.1.4.8 The -F Switch 314

8.1.4.9 The -G Switch 314

8.1.4.10 The -H Switch 314

8.1.4.11 The -i Switch 315

8.1.4.12 The -I Switch 315

8.1.4.13 The -k and -K Switches 315

8.1.4.14 The -l and -L Switches 315

8.1.4.15 The -n Switch 315

8.1.4.16 The -O Switch 316

8.1.4.17 The -p and -P Switches 317

8.1.4.18 The -q Switch 317

8.1.4.19 The -r and -R Switches 318

8.1.4.20 The -s and -S Switches 318
8.1.4.21 The -T Switch 318
8.1.4.22 The -U Switch 318
8.1.4.23 The -v and -V Switches 318
8.1.4.24 The -W Switch 318
8.1.4.25 The -X and -x Switches 319
8.1.4.26 The -y Switch 319
8.1.4.27 The -Z Switch 319
8.1.5 Network Intrusion Detection System Mode 319
8.2 Using SpywareBlaster 322
8.2.1 Obtaining the Program 323
8.2.2 Adding Protection 325
8.2.2.1 Restricted Site Protection 327
8.2.2.2 System Snapshot 328
8.2.3 The Tools Menu 329
8.2.3.1 Flash Killer 330
8.2.3.2 Custom Blocking 331
8.2.4 Checking for Updates 331
8.3 Using Online Armor 332
8.3.1 Installation 332
8.3.2 Operation 335
8.4 AXCrypt File Encryption 338
8.4.1 Installation 340
8.4.2 Operation 340

CHAPTER 9 ENHANCING NETWORK PERFORMANCE 345
9.1 Third-Party Networking Tools 345
9.1.1 Bandwidth Tools 346
9.1.2 IP Tools 347
9.1.3 Miscellaneous Networking Tools 348
9.1.4 Network Information 349
9.1.5 Other Sites to Consider 349
9.1.6 Using Search Tools 350
9.2 Windows Built-In Networking Tools 352
9.2.1 Disk Cleanup 352
9.2.2 Why Disk Defragmentation Matters 354
9.2.3 Resource Monitor 355
9.2.4 System Information 358

INDEX 361